1:25-mj-01005-JMC

ATTACHMENT A-2

(Apple iCloud Account Associated with Apple ID dkmartin323@gmail.com)

DESCRIPTION OF THE ITEM(S) TO BE SEARCHED

The items to be searched is information and content from the Apple iCloud Account associated with the following identifiers ("**Apple Account**") that that are stored at premises owned, maintained, controlled, or operated by Apple, Inc., a business with offices located at One Apple Park Way, MS: 169-5CLP, Cupertino, CA 95014:

- Apple ID: dkmartin323@gmail.com

ATTACHMENT B-2
(Apple iCloud Account Associated with Apple ID dkmartin323@gmail.com)

I. Files and Accounts to be produced by Apple Inc.

Apple Inc. (Apple) shall disclose responsive data, if any, by sending it to Federal Bureau of Investigation, ATTN: SA Richard Gianforcaro, 2600 Lord Baltimore Drive, Windsor Mill, Maryland, 21244, using the US Postal Service or another courier service, or by other secure electronic means to rcgianforcaro@fbi.gov, notwithstanding 18 U.S.C. Sec. 2252A or similar statute or code.

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Apple, including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Apple, or have been preserved pursuant to prior preservation requests made (Apple reference numbers 202400905597 and 202501079851), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A-2 from the date of account creation until present time:

1. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

2. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

3. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments);

4. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at

which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

5. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

6. The activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

7. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

8. All records pertaining to the types of service used;

9. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken;

10. All device registration information, all customer service records, all iTunes records, all Apple retail store transactions, all Apple online store transactions, all Apple and iTunes gift card transactions, all iCloud subscriber information, mail logs, and other transactional data, all Find My iPhone connection logs and transactional activity, all Apple device MAC addresses, all Apple Game Center connection logs and transactional records; all iOS device activation records; all Dual SIM, nano SIM, and eSIM records and carrier information, all Apple account sign-on and connection logs, all My Apple ID and iForgot connection logs and transactional records, and all iMessage capability query logs;

11. All accounts linked to the accounts listed in Attachment A-2, including accounts linked by Apple or third-party cookies, SMS number, or secondary or recovery emails, or other account-linking methods available to Apple, and to any accounts for which the accounts in Attachment A-2 are the secondary or recovery email address;

12. All location history with associated timestamps;

13. All search history with associated timestamps;

14. All accounts linked to the accounts in Attachment A-2, including accounts linked

by Apple or third-party cookies, SMS number, Internet Protocol Address, secondary or recovery emails, or other account-linking methods available to Apple, and to any accounts for which the accounts in Attachment A-2 are the secondary or recovery email address.

II. Information to be Seized by Law Enforcement Personnel

The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18 U.S.C. § 2251(a) (sexual exploitation of children), 18 U.S.C. § 2422(b) (coercion and enticement of a minor), 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), among other federal criminal statutes, (the "Target Offenses"), including but not limited to:

15. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under 18 U.S.C. § 2256(8);

16. Any and all correspondence identifying persons producing, transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2252A(a)(5)(B) & (b)(2), 2256(2);

17. Any and all records, documents, invoices and materials that concern any accounts with Internet Service Providers, screen names, online accounts, cellular accounts, websites, or email accounts;

18. Any and all visual depictions of minors, to include depictions of minors engaged in sexually explicit conduct, nude pictures, and modeling;

19. Any visual depiction of blankets, sheets, clothes, etc., bearing resemblance to items observed in the images/videos referenced in the affidavit.

20. Images depicting the interior or exterior of residences, public establishments, and vehicles;

21. Any and all documents relating to the purchase of digital cameras, including "spy" cameras, cell phones with cameras and/or internet capability, or other photographic equipment.

22. Any and all documents, records, or correspondence pertaining to occupancy, ownership or other connection to the device.

23. Any and all diaries, notebooks, notes, address books, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors;

24. Any and all financial documents, records, receipts, credit card statements, and/or correspondence relating to payments sent and/or received in connection with minors engaged in

sexually explicit conduct, nude pictures, modeling, and/or hosting websites;

25. All images, messages, and communications regarding methods to avoid detection by law enforcement:

26. Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to:

a. Correspondence with children;
b. Any and all visual depictions of minors;
c. Internet browsing history;
d. Books, logs, emails, chats, diaries and other documents.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **(pages/CDs/megabytes)**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature